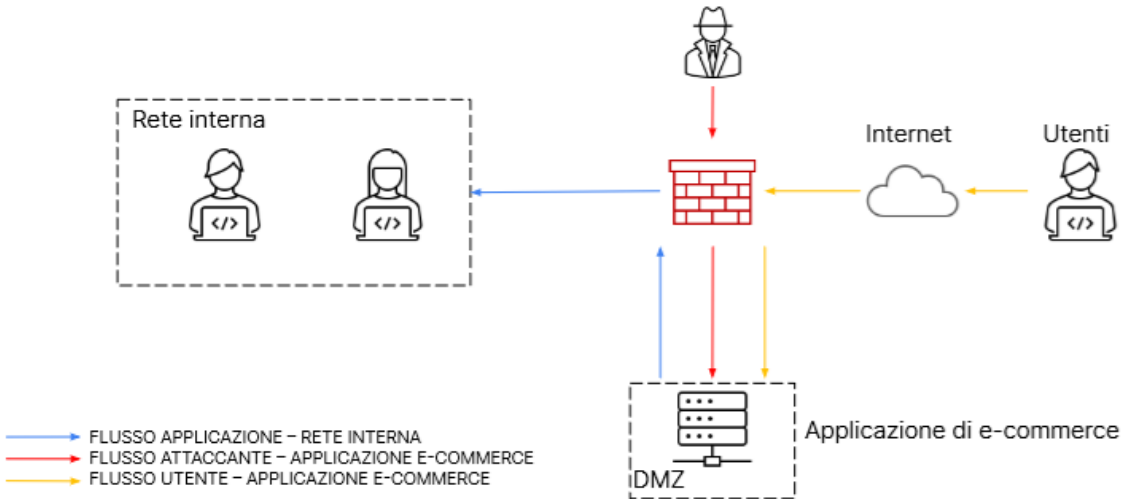
Progetto settimanale

Attacco all'e-commerce – Interventi di prevenzione e incident response

1. Azioni preventive

Nella figura seguente viene raffigurata un'ipotetica situazione di attacco alla piattaforma e-commerce da parte di un attaccante esterno.



L'azione preventiva più efficace, utile al fine di difendere l'applicazione web da attacchi di SQLi injection o XSS da parte di un ipotetico attaccante, è quella di implementare la rete ponendo un Web Application Firewall (WAF) all'ingresso della DMZ (Demilitarized zone). Il WAF filtra le richieste dannose a un'applicazione Web e offre maggiore visibilità sulla provenienza del traffico; allo stesso tempo, però, consente agli utenti di continuare ad accedere alle applicazioni Web come previsto.

In questo modo, l'attaccante sarebbe bloccato dal WAF, che impedirebbe il suo accesso all'interno della DMZ e l'esecuzione dell'eventuale attacco.

Nella figura 1 di seguito vediamo l'implementazione del WAF.

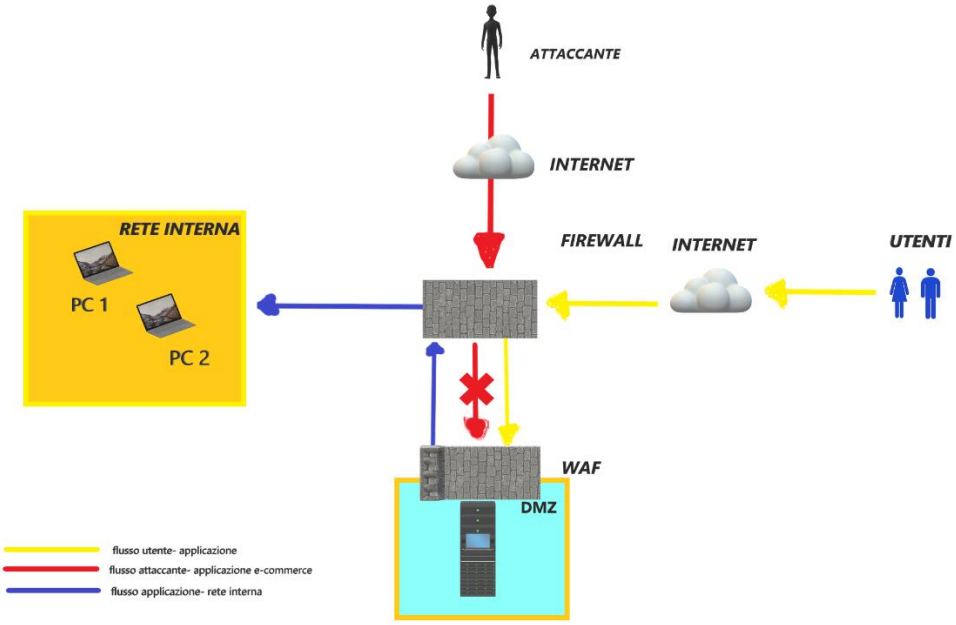


Figura 1

2. Business Impact Assessment (BIA)

Poniamo il caso in cui l'applicazione Web subisce un attacco di tipo Ddos dall'esterno che rende l'applicazione non raggiungibile per **10 minuti.** Considerando che **ogni minuto gli utenti spendono 1.500 euro** sulla piattaforma di e-commerce, possiamo convenire che l'impatto del business in questo caso sarà pari al prodotto della spesa per il tempo di non raggiungibilità dell'e-commerce.

Il calcolo effettuato è il seguente: 1.500x10=15.000 €

L'impatto sul business sarà pari a 15.000 di perdita per una disconnessione del servizio di 10 minuti.

3. Incident Response

Tenendo presente la situazione iniziale, l'attaccante riesce ad accedere alla DMZ e infetta l'E-commerce con un malware.

Immaginando una situazione in cui non si è interessati a rimuovere l'accesso da parte dell'attaccante ma comunque si voglia preservare la rete evitando di propagare il malware, possiamo pensare di "isolare" la DMZ da eventuali comunicazioni con la rete interna.

Nello stesso tempo, però, l'accesso ad Internet verrà mantenuto, per consentire all'attaccante di continuare il suo attacco e agli utenti di continuare ad usufruire del servizio di e-commerce.

Questa è una tecnica non troppo aggressiva che ci permette di osservare l'attaccante e di studiare le sue mosse, prima di rimuovere del tutto il malware. In più, questa tecnica ci permette comunque di tenere attivo il sito e di controllare gli ingressi attraverso il firewall posto al centro della rete.

La figura 2 di seguito ci mostra la situazione di isolamento della DMZ rispetto alla rete interna.

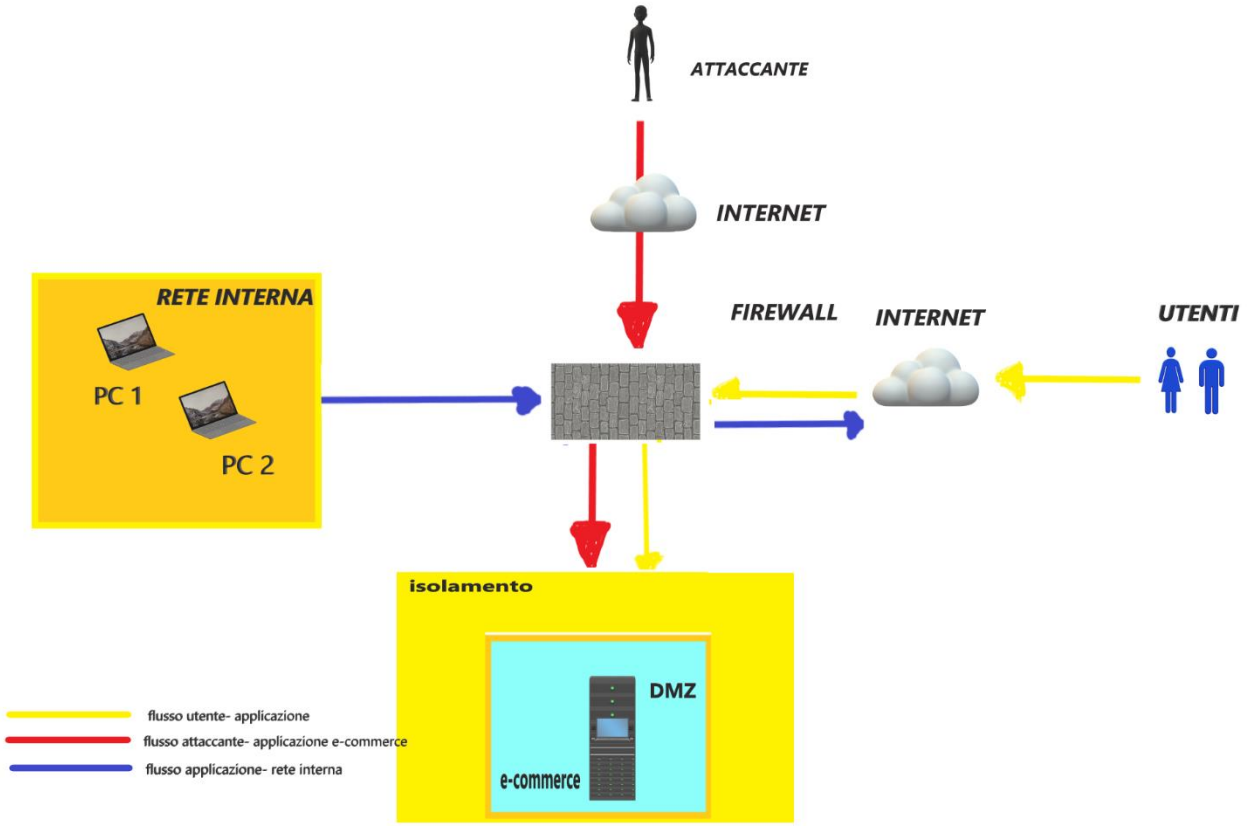


Figura 2

4. Soluzione completa e modifiche

La soluzione completa sarebbe quella di avere già a disposizione dell'e-commerce un WAF per poter filtrare le comunicazione dall'esterno in maniera più dettagliata e bloccare così l'attaccante.

In più, si potrebbe aggiungere un honeypot, prima del server di e-commerce così da riuscire a trarre in inganno il possibile attaccante, che verrebbe reindirizzato all'interno di una trappola che ci aiuterà a proteggere il sito di e-commerce.